A5 - Sécurité Réseau

Sécurisation d'un serveur Linux, Internet ou Intranet

Objectifs

- Savoir déployer et utiliser des outils de sécurisation et de test sur plate-forme Linux

Matériel

- Un PC par stagiaire
- Support de cours

Pré-requis

- Connaissance de Linux et de l'administration réseau (niveau cours A2)
- Maîtrise de la gestion de l'arborescence du système
- Maîtrise d'un éditeur de fichier texte

Environnement du cours

- Cours théorique
  - Support de cours au format PDF (en anglais) et une version imprimée lors des sessions en présentiel
  - Cours dispensé via le système de visioconférence Teams (si à distance)
  - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique
- Au début de chaque demi-journée une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Plan du cours

Sécurisation des accès

- Notions de base sur TCP/IP
- Parefeu Netfilter/iptables, zone démilitarisée (DMZ), gestion avec fwbuilder
  - Installation de iptables et fwbuilder
  - Les directives définissant les règles
  - Configuration de base pour faire du routage
  - Configuration de base pour faire du filtrage
  - La translation d'adresse NAT
  - La gestion des règles avec fwbuilder

Communications sécurisées

- OpenSSL
  - Installation
  - Création des certificats pour un client ou un serveur

- Accès distant avec OpenSSH
  - Installation/configuration du serveur OpenSSH
  - Installation/configuration du client SSH Linux ou Windows
- Mise en place de réseaux privés virtuels (VPN) avec FreeSWAN et IPsec
  - Installation/Configuration
  - Liaison entre sites
  - Liaison entre un site et des portables (Road Warrior)

Administration de la sécurité

- Détection d'intrusion (IDS) avec SNORT sur Linux
  - Installation de SNORT
  - Configuration
  - Suivi des logs
  - Ecriture des règles
- Supervision du réseau avec NAGIOS
  - Installation/configuration de NAGIOS
  - Les plugins
  - Analyse du réseau
  - Suivi des éléments actifs du réseau
- Outils de surveillance réseau : hping, ethereal, tcpdump, nmap, netcat
  - Installation
  - Utilisation de ces outils pour analyser le fonctionnement du réseau